CLAIMS

1. (PREVIOUSLY PRESENTED) A system for controlling access to digital services comprising:

(a) a control center configured to coordinate and provide digital services;

(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;

(c) the satellite configured to:

(i) receive the digital services from the uplink center;

(ii) process the digital services; and

(iii) transmit the digital services to a subscriber receiver station;

(d) the subscriber receiver station configured to:

(i) receive the digital services from the satellite;

(ii) control access to the digital services through an integrated receiver/decoder (IRD);

(e) a conditional access module (CAM) communicatively coupled to the (IRD), wherein the CAM comprises:

(i) a system bus;

(ii) a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to the digital services is distributed among the nonvolatile memory components wherein separate and independent attacks must be conducted on each nonvolatile memory component to gain unauthorized access to the digital services; and

(iii) a microprocessor communicatively coupled to the nonvolatile memory components, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

2. (ORIGINAL) The system of claim 1, wherein the conditional access module is a smart card.

3. (ORIGINAL) The system of claim 2, wherein the smart card further comprises:
a volatile memory component;
a custom logic block; and
a system input/output module.

4. (CANCELLED)

5. (ORIGINAL) The system of claim 1, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

6. (ORIGINAL) The system of claim 1, wherein the plurality of nonvolatile memory components reside on a single chip.

7. (ORIGINAL) The system of claim 6, wherein a charge pump is shared between the plurality of nonvolatile memory components.

8. (ORIGINAL) The system of claim 6, wherein programming control is shared between the plurality of nonvolatile memory components.

9. (ORIGINAL) The system of claim 1, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

10. (ORIGINAL) The system of claim 1, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

11. (ORIGINAL) The system of claim 1, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

12. (PREVIOUSLY PRESENTED) A method of controlling unauthorized access to digital services comprising:

distributing access to digital services among a plurality of physically separate and independently controlled nonvolatile memory components on a system bus wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and

communicatively coupling the plurality of nonvolatile memory components to a microprocessor, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

13. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components are contained within a security component known as a smart card.

14. (ORIGINAL) The method of claim 13, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

15. (ORIGINAL) The method of claim 13, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

16. (CANCELLED)

17. (ORIGINAL) The method of claim 12, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

18. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components reside on a single chip.

19. (ORIGINAL) The method of claim 18, wherein a charge pump is shared between the plurality of nonvolatile memory components.

20. (ORIGINAL) The method of claim 18, wherein programming control is shared between the plurality of nonvolatile memory components.

21. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

22. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

23. (ORIGINAL) The method of claim 12, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

24. (PREVIOUSLY PRESENTED) A method of accessing digital services comprising:

storing state information in a plurality of nonvolatile memory components, wherein the plurality of nonvolatile memory components are physically separate and independently controlled, wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services;

accessing digital services using the nonvolatile memory components wherein the state information is used to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

25. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components are contained within a security component known as a smart card.

26. (ORIGINAL) The method of claim 25, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

27. (ORIGINAL) The method of claim 24, wherein a single microprocessor controls the nonvolatile memory components.

28. (CANCELLED)

29. (ORIGINAL) The method of claim 24, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

30. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components reside on a single chip.

31. (ORIGINAL) The method of claim 30, wherein programming control is shared between the plurality of nonvolatile memory components.

32. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

33. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

34. (ORIGINAL) The method of claim 24, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

35. (PREVIOUSLY PRESENTED) A conditional access module (CAM), comprising:

a system bus;

a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to digital services is distributed among the nonvolatile memory components, and wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and

a microprocessor communicatively coupled to the nonvolatile memory components, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

36. (ORIGINAL) The CAM of claim 35, wherein the conditional access module is a smart card.

37. (ORIGINAL) The CAM of claim 36, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

38. (ORIGINAL) The CAM of claim 36, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

39. (CANCELLED)

40. (ORIGINAL) The CAM of claim 35, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

41. (ORIGINAL) The CAM of claim 35, wherein the plurality of nonvolatile memory components reside on a single chip.

42. (ORIGINAL) The CAM of claim 41, wherein a charge pump is shared between the plurality of nonvolatile memory components.

43. (ORIGINAL) The CAM of claim 41, wherein programming control is shared between the plurality of nonvolatile memory components.

44. (ORIGINAL) The CAM of claim 35, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

45. (ORIGINAL) The CAM of claim 35, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

46. (ORIGINAL) The CAM of claim 35, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

47. (PREVIOUSLY PRESENTED) An article of manufacture for preventing unauthorized access to digital services comprising:

means for distributing access control to digital services among a plurality of physically separate and independently controlled nonvolatile memory components on a system bus, and wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and

means for communicatively coupling the plurality of nonvolatile memory components to a microprocessor, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

48. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components are contained within a security component known as a smart card.

49. (ORIGINAL) The article of manufacture of claim 48, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

50. (ORIGINAL) The article of manufacture of claim 48, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

51. (CANCELLED)

52. (ORIGINAL) The article of manufacture of claim 47, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

53. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components reside on a single chip.

54. (ORIGINAL) The article of manufacture of claim 53, wherein a charge pump is shared between the plurality of nonvolatile memory components.

55. (ORIGINAL) The article of manufacture of claim 53, further comprising means for sharing programming control between the plurality of nonvolatile memory components.

56. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

57. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

58. (ORIGINAL) The article of manufacture of claim 47, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

59. (PREVIOUSLY PRESENTED) The system of claim 1, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) the CAM further comprises a microprocessor's unprotected nonvolatile memory component wherein the microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

60. (PREVIOUSLY PRESENTED) The method of claim 12, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

61. (PREVIOUSLY PRESENTED) The method of claim 24, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

62. (PREVIOUSLY PRESENTED) The CAM of claim 35, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) the CAM further comprises a microprocessor's unprotected nonvolatile memory component wherein the microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

63. (PREVIOUSLY PRESENTED) The article of manufacture of claim 47, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.